Freedom House

FREEDOM ON THE NET 2024

# China

NOT FREE

**9** /100

| | |
|---|---|
| **A.** Obstacles to Access | **7** /25 |
| **B.** Limits on Content | **2** /35 |
| **C.** Violations of User Rights | **0** /40 |

LAST YEAR'S SCORE & STATUS

**9** /100 **Not Free**

Scores are based on a scale of 0 (least free) to 100 (most free). See the research methodology and report acknowledgements.

# Key Developments, June 1, 2023 – May 31, 2024

Chinese internet users have faced the world's worst conditions for internet freedom for a decade. People face severe legal and extralegal repercussions for online activities like sharing news stories, talking about their religious beliefs, and communicating with family members and others overseas. Authorities wield immense power over the technology industry, deploying regulatory investigations and removal orders to enforce government narratives.

- Authorities restricted access to anticensorship tools, blocking access to "unauthorized" virtual private networks (VPNs) and penalizing people who used them (see B1 and C3).
- Censors systematically scrubbed criticism of the government from the internet, including expressions of grief and other commentary after the unexpected death of former premier Li Keqiang in October 2023 (see B2).
- New rules for self-media accounts—independent writers, bloggers, and social media celebrities—were introduced in July 2023, including real-name registration requirement for accounts with over 500,000 followers. The new rules prompted some individuals to close their accounts (see B6 and C4).
- Independent filmmaker Chen Pinlin was detained in November 2023 after posting online a documentary with footage of the historic White Paper protests of the previous year. He faces up to five years in prison (see B8 and C3).
- Sun Lin, an activist and journalist, died from injuries after a November 2023 police raid. He had posted online about videos of anti–Xi Jinping protests in the hours before the raid (see C7).

# Political Overview

China's authoritarian regime has become increasingly repressive in recent years. The ruling Chinese Communist Party (CCP) continues to tighten control over all aspects of life and governance, including the state bureaucracy, the media, online speech, religious practice, universities, businesses, and civil society associations.

Following a multiyear crackdown on political dissent, independent nongovernmental organizations (NGOs), and human rights defenders, China's civil society has been largely decimated.

*Note: Tibet and Hong Kong are not covered in this report. Certain territories that are assessed separately in Freedom House's* Freedom in the World *report are excluded from the relevant country reports in* Freedom on the Net*, as conditions in such territories differ significantly from those in the rest of the country.*

# A. Obstacles to Access

**A1** 0-6 pts

| **Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?** | **5**/6 |
|---|---|

According to the government's China Internet Network Information Center (CNNIC), there were 1.09 billion internet users in China—representing 77.5 percent of the population—as of December 2023. That figure represents an increase of 25 million since December 2022. Some 99.9 percent of users access the internet via mobile devices. [1]

Chinese internet users can access high-speed services, though connection speeds are slowed by the country's blocking and filtering apparatus), which filters all cross-border traffic and makes the loading of content from foreign-hosted websites sluggish (see B1). [2] According to the analytics company Ookla, the median mobile download speed stood at 135.71 megabits per second (Mbps) in June 2024. The median fixed-line broadband download speed was 223.57 Mbps. [3] Internet speeds vary significantly in different parts of the country. According to government data, the fastest available connections were in Shanghai, and the slowest were in less prosperous and more heavily censored regions, such as the Xinjiang Uygur Autonomous Region. [4]

Chinese companies have been at the forefront of building and deploying fifth-generation (5G) mobile networks. In January 2024, the Ministry of Industry and Information Technology (MIIT) reported that China had 3.38 million 5G base stations, and 805 million 5G subscribers as of the end of 2023. [5]

**A2** 0-3 pts

| **Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?** | **1** / 3 |
|---|---|

Internet access is relatively affordable for the average user, but other digital divides limit access for certain populations.

According to the China Academy of Information and Communication Technology, fixed-line broadband services cost an average of 35.8 yuan ($5.08) in the first three quarters of 2023, while mobile users paid an average of 2.25 yuan ($0.37) per gigabyte (GB). [6]

The urban-rural digital divide narrowed during the coverage period, according to government figures. Internet penetration in cities was 83.3 percent as of December 2023, compared to 66.5 percent in rural areas. [7] Some 317 million people did not have internet access as of that month, 51.8 percent of them in rural areas. [8]

The shutdown of 2G networks in by Guangdong Telecom in August 2023 in the province led to some users losing connection unless they purchased new devices and packages. [9] Approximately 17 percent of all mobile phone users, or 273 million people, use 2G networks as of 2020 according to the MIIT. [10]

**A3** 0-6 pts

| **Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?** | **1** / 6 |
|---|---|

The government maintains control over China's gateways to the global internet, giving authorities the ability to restrict connectivity or access to content hosted on servers outside the country. [11] This arrangement is the foundation for the "Great Firewall," the informal name for the government's comprehensive internet censorship system. All service providers must subscribe via the gateway operators, which are overseen by the Ministry of Industry and Information Technology (MIIT).

Human rights activists and their families are subject to targeted disconnections. For example, in February 2023, a month ahead of China's annual legislative sessions, authorities disabled internet service for Wuhan-based activist Xu Wu and his family. [12]

The government has cut internet access in response to specific events, though authorities have relied more on other censorship tactics in recent years. In late May 2023, authorities reportedly cut off the internet in several neighborhoods in Yunnan Province following an altercation between ethnic Hui Muslims and police outside a mosque. [13] The most dramatic example occurred in 2009, when authorities imposed a 10-month internet disruption in Xinjiang—home to 25.9 million people according to the 2020 census—after ethnic violence in the regional capital, Urumqi. [14]

Network shutdowns are often explained as national security precautions. The cybersecurity law and Article 84 of a 2015 antiterrorism law introduced fines and detentions of up to 15 days for telecommunications firms and ISPs, as well as relevant personnel, who fail to restrict certain forms of content including "shut[ting] down related services" (see B3 and C2). [15] Under a revised cybersecurity rule implemented in February 2022, government agency must conduct a national security review of the purchases of network products and services made by "critical information infrastructure operators." [16]

**A4** 0-6 pts

| **Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?** | **0** / 6 |
|---|---|

The state controls the internet service provider market through legal and regulatory measures. State-owned China Mobile, China Telecom, and China Unicom dominate the mobile market, [17] though the government has occasionally authorized new players to enter the market. [18] China Mobile dominates the mobile and fixed-line broadband markets, with 991 million and 264 million subscribers, respectively, as of December 2023. [19] China Telecom reported 408 million mobile subscribers and 190 million fixed-line broadband subscribers as of December 2023, [20] while China Unicom reported 333 million mobile subscribers and 113 million fixed-line broadband subscribers. [21]

Authorities exercise tight control over cybercafés and other public access points, which are licensed by the Ministry of Culture in cooperation with other state entities. [22] Video gamers continue to gather at cybercafés regularly. Some 132,000 cybercafés were active as of June 2023. [23]

**A5** 0-4 pts

| | |
|---|---|
| **Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?** | **0** / 4 |

Several government agencies and CCP bodies are responsible for internet regulation at the local and national levels, but the system has been consolidated during Xi Jinping's tenure.

The Cyberspace Administration of China (CAC) [24] and the CCP's Central Cyberspace Affairs Commission (CCAC) oversee the telecommunications sector and regulate internet content. [25] The 2017 cybersecurity law identifies the CAC as the principle agency responsible for implementing many of its provisions. [26] The CAC reports to the CCAC, which is headed directly by Xi. [27] Since 2014, the CCAC has also overseen the CNNIC, an administrative agency under the MIIT that issues digital certificates to websites. [28]

The CCP has exerted greater control over the press, film, radio, and television industries in recent years, including online video and streaming services. Since an administrative restructuring occurred in March 2018, more agencies involved in media regulation, including online content, have been directly subordinated to the CCP's Central Propaganda Department, although several continue to report to the State Council. [29] Zhuang Rongwen has served as CAC director since mid-2018 [30] and continued in that position during the coverage period, while simultaneously serving as deputy director of the Central Propaganda Department. [31]

# B. Limits on Content

**B1** 0-6 pts

| | |
|---|---|
| **Does the state block or filter, or compel service providers to block or filter, internet content, particularly material that is protected by international human rights standards?** | **0** / 6 |

The Great Firewall is the world's most sophisticated internet censorship apparatus. Content that contains criticism of individuals, policies, or events that are considered integral to the one-party system is blocked. The breadth of censorship leaves Chinese users with a highly controlled, monitored, and manipulated version of the internet. The censorship monitoring platform GFWatch identified over 200,000 blocked domains as of the end of the coverage period. [32] Long-standing blocks on international communications platforms have helped to enable the growth of local products, such as messaging service WeChat and microblogging platform Sina Weibo, which are legally required to comply with government's strict censorship rules (see B2).

According to GreatFire.org—an anticensorship group that tracks filtering in China—as of February 2024, over 100,000 websites were blocked in China. [33] Many international news outlets and their Chinese-language websites are blocked, such as those of the *New York Times*, Reuters, the *Wall Street Journal*, the Australian Broadcasting Corporation (ABC), and the British Broadcasting Corporation (BBC). The websites of independent Chinese-language news services from Taiwan, Hong Kong, and the Chinese diaspora—such as the *Liberty Times* in Taiwan, Initium in Singapore, and the China Digital Times in the United States—remained blocked during the coverage period. The websites of human rights groups such as Amnesty International, Human Rights Watch (HRW), and Freedom House are also blocked.

Most international social media and messaging platforms are blocked, including Facebook, WhatsApp, Twitter, Instagram, Signal, Clubhouse, YouTube, Telegram, Snapchat, Line, and Pinterest. [34] The popular discussion forum Reddit was blocked in August 2018, [35] while all languages of Wikipedia were blocked in April 2019. [36] A number of Google services—including Maps, Translate, Calendar, Docs, Drive, Scholar, and Analytics—remained blocked as of the end of the coverage period. A localized version of Duolingo became accessible in June 2022, after the app was blocked in August 2021. [37]

Blocks on global search engines severely limit the content available on the Chinese internet. Google's search engine has been blocked since 2012, [38] while the Yahoo search function was blocked in 2018. [39]

People outside of China are increasingly restricted from accessing sites inside China. For a brief period in November 2022 and permanently since September 2023, non-Chinese IP addresses have been blocked from accessing the Supreme People's Court website. [40] Similar restrictions have been observed on other government websites. [41] According to the German research hub MERICS, the increased restrictions on foreign access to the Chinese internet are implemented through a number of measures, including geoblocks, restrictions on encrypted and VPN web traffic, and social media account registration rules that require Chinese phone numbers. [42]

A minority of Chinese internet users, though they number in the tens of millions, access blocked websites with circumvention tools like VPNs (see B7). However, the government has intensified its restrictions on these tools since 2017, when the MIIT banned the use of unlicensed VPNs. [43] Service providers are barred from setting up VPNs without government approval, and illegal VPN operations have been increasingly targeted for closure or blocking (see C3). [44] Blocks on VPNs typically escalate ahead of high-profile events, such as annual plenary sessions of the Chinese legislature. [45] VPN providers have noted that a growing technical sophistication of Chinese authorities has been reflected in VPN blocking incidents. [46] In November 2021, the CAC released a draft regulation, titled Network Data Security Management Regulations, that would punish individuals and institutions for helping users circumvent internet censorship. Presumably targeting app stores and hosting sites, the regulations would provide for penalties of up to 500,000 yuan ($70,300). [47]

In October 2022, Chinese censors imposed more restrictions on circumvention tools, mainly affecting transport layer security (TLS)–based programs, according to the Great Firewall Report, a censorship monitoring platform. It was reportedly the largest-scale block of TLS-based tools, which are widely used by Chinese internet users, to date. [48]

**B2** 0-4 pts

| **Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content, particularly material that is protected by international human rights standards?** | **0** / 4 |
| --- | --- |

The government requires locally hosted websites, social media platforms, and other technology companies to proactively monitor and remove significant amounts of banned content and accounts. They can face severe punishment for failure to comply.

The scale of content removals, website closures, and social media account deletions continued to expand during the coverage period, reaching new types of platforms and extending to topics that were previously uncensored. Censored topics often involve news, commentary, or criticism related to government policies, the CCP, and foreign affairs, as well as content related to health, safety, civil society, and public protest. **49** Content that violates long-standing taboos is consistently and systematically censored, including content related to the June 4, 1989, Tiananmen Square massacre; **50** Taiwanese affairs; and the government's repression of marginalized communities like ethnic minorities in Xinjiang and Tibet and Falun Gong and Christian religious practitioners. Uyghur- and Tibetan-language content specifically is often targeted for removal. **51**

The CAC regularly launches "rectification" and "clean-up" campaigns to pressure websites and social media platforms to more effectively police content. In early 2024, the CAC announced it had shut down 14,624 "illegal" websites, removed 259 apps, and had 127,878 accounts on social media platforms shut down in 2023. **52** The Ministry of Public Security has declared 2024 a year of "special operations" against online rumors. **53** Censors have also increasingly targeted "self-media," a category that includes independent writers, bloggers, and social media celebrities (see B6). Over 66,600 self-media accounts have been shut down in 2023. **54** In June 2023, Weibo banned a finance writer with 4.7 million followers for commenting on economic issues. **55**

Authorities pressure Chinese internet companies to tightly enforce censorship regulations or risk suspensions, fines, blacklisting, closure, or even criminal prosecution of relevant personnel. This has intensified under the cybersecurity law that took effect in 2017. The CCP's Central Propaganda Department and its local subsidiaries issue regular instructions to news sites and social media platforms on what to restrict. **56** The CAC announced in January 2024 it had imposed administrative penalties on companies including Baidu, Quark Browser, Douyin, Sina Weibo, and Wechat for failing to sufficiently censor content. **57**

International companies also respond to censorship demands or pressure from the authorities to restrict online content. In October 2022, Google closed its Translate service in China. [58] Grindr, an LGBT+ dating app, removed itself from Chinese app stores in February 2022, citing a new privacy law. [59] Similarly, LinkedIn shut down its service in China in October 2021. [60] Microsoft Bing's search engine operates a heavily censored version in China, with stricter restrictions on political and religious content than its Chinese competitor Baidu, according to analysts at the Citizen Lab, a research group at the University of Toronto. [61]

Apple has removed or otherwise restricted apps due to regulatory and political pressure in recent years. App store monitor AppleCensorship reported that over 16,000 apps were unavailable on Apple's app store in China, out of 56,400 tested, as of October 2024, [62] including hundreds of VPN services. [63] In April 2024, the CAC ordered Apple to remove the apps for WhatsApp, Threads, Telegram, and Signal for the China App store. [64] Apple has also removed or restricted iOS features, including private relay, eSIMs, and links for video calls for users in China. [65] In November 2022, Apple restricted the use of AirDrop, a file-sharing feature on iPhones, [66] after Shanghai subway passengers used it to spread messages about a lone protester on a bridge in Beijing. [67]

Security officials continued to harass and coerce users to delete content, particularly from X (formerly Twitter), which is blocked in China. A small but savvy community of internet users access X via circumvention tools, enabling participation in conversations that are heavily censored within the Great Firewall, including on protests (see B8). Over the past several years, numerous users faced reprisals for their Twitter activities, including prison time, with many forced to delete their posts en masse (see C3 and C7). [68]

Content that mocks or in some case simply discusses Chinese leaders, particularly President Xi, is strictly censored. According to a leaked list from CAC, 35,467 different phrases linked to President Xi were blocked online since 2016. [69] Following the unexpected death of former Chinese premier Li Keqiang in October 2023, censors removed content that expressed grief. Posts and accounts that referenced a song that was widely interpreted as an oblique critique of Xi, were deleted or suspended. [70] In July 2023, a month after the then foreign minister

Qin Gang disappeared from public attention, all references to him on the foreign ministry's website were removed, though some were later reinstated. [71]

Content is often removed around major political events. Ahead of the March 2023 annual "Two Sessions" meetings, online comments on the approval of a third presidential term for Xi Jinping were systematically deleted. [72] Freedom House research released in August 2023 found that almost 20 percent of a sample of 4,170 Sina Weibo posts with dissent-related language were removed. [73]

Censors remove content connected to social, economic, and health issues. In the aftermath of unprecedented dissent against the government's zero COVID-19 policies in 2022, censors deleted a vast amount of viral content, [74] (see B8) and the government ordered social media companies to hire more censors and to scrub references to circumvention technology. [75] After lockdown rules were dropped in response to the protests, Sina Weibo censored search results for the topic "pandemic in Beijing," preventing real-time discussions on the ensuring impact. [76] Censorship on COVID-19 information continued in July 2023 with censors removing a Caixin report highlighting a surge in cremation following the lifting of lockdown in Zhejiang Province, [77] and the data expunged from the provincial government's website. [78] During the pandemic, censorship of content discussing zero-COVID was particularly stringent in areas with large ethnic minority populations. [79]

Since the Chinese government declared victory in eradicating absolute poverty at the end of 2020, online content that depicted poverty was frequently censored. In October 2022, streaming sites removed *Return to Dust*, a film on poverty. The name of the film was also censored on Sina Weibo. [80] Content that otherwise reflects struggles within the Chinese economy were also censored. The social media accounts of influential financial writer Wu Xiaobo were removed after he critically compared the Chinese and US technology sectors. [81]

LGBT+ and women's rights content continues to be censored on China's internet." [82] In August 2023, Sina Weibo took down several prominent LGBT+ accounts. [83] The social media accounts of two K-pop stars with hundreds of millions of followers were banned in November 2023 after they posted material from a burlesque show. [84] In September 2021, the National Radio and Television Administration (NRTA) ordered broadcasters and the entertainment industry to

ban “sissy men,” prompting a wave of content removals on social media platforms. [85]

Foreign governments’ official accounts were also censored, especially when discussing human rights and political topics. In February 2023, a translated excerpt of US president Joe Biden’s State of Union address published by the US Embassy WeChat account was blocked. [86] In July and September 2022, Sina Weibo posts from the UK and US embassies, respectively were deleted after discussing developments in Hong Kong [87] and Xinjiang. [88]

Developers of censorship circumvention tools have also faced pressure to remove or restrict access to their services. In November 2023, a proxy software, Clash for Windows, was deleted from GitHub by its developer, who some suspected had been pressured by the government. [89]

Large language model (LLM)–based chatbots were also subjected to censorship during the coverage period. [90] In February 2023, Chinese regulators told technology firms in the country to discontinue access to ChatGPT and to disclose their own plans to develop AI-driven chatbots. [91] The founder of ChatYuan, an AI chatbot, said that the chatbot would “filter certain keywords” with more layers of review than might be expected overseas. [92]

Automation technology is playing an increasing role in censorship. In August 2019, Citizen Lab revealed the existence of image-filtering capabilities on WeChat, which targeted users’ creative efforts to circumvent text-based censorship through image-based commentary. [93] Alibaba, Tencent, ByteDance, and the People’s Daily are industry leaders in content moderation and censorship technologies that intentionally target political content, selling the systems to other Chinese companies as well as foreign clients. [94]

**B3** 0-4 pts

| **Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?** | **0** / 4 |
|---|---|

Censorship decisions are arbitrary, opaque, and inconsistent because the nation’s rule of law is weak and because of the number of actors and processes involved. Regulations issued by government and CCP agencies establish censorship

guidelines and cover vaguely defined restrictions which are left open to wide interpretation. The impact of content restrictions may vary depending on factors like timing, technology, and geographic region. ISPs reportedly install filtering devices differently, including in the internet backbone or even in provincial-level internal networks. [95] Lists of prohibited websites and sweeping censorship directives are closely held secrets but are periodically leaked. There are no formal avenues for appeal, and directives cannot be challenged in the courts. Criticism of censorship is itself censored. [96] There is no transparency surrounding private companies' day-to-day censorship in China, and users similarly lack avenues for appeal.

The cybersecurity law, in effect since 2017, provides legal grounds for officials to instruct network operators to stop the transmission of certain content to protect public security, among other restrictions (see A3). Proposed amendments in 2022 would increase penalties and bring the law in line with other legislation introduced since its enactment, including the Personal Information Protection Law. [97] Article 84 of a 2015 antiterrorism law introduced fines and detentions of up to 15 days for telecommunications firms and ISPs, as well as relevant personnel, who fail to "stop transmission" of terrorist or extremist content; "shut down related services;" or implement "network security" measures to prevent the transmission of such content (see C2). [98]

The CAC and other bodies routinely introduce new rules and guidelines to further refine online restrictions, with an increasing focus on user-generated content. In August 2023, the CAC introduced new rules to require websites to accept and handle reports of online "infringement" towards enterprises, such as counterfeit, misleading or rumors information. [99] A June 2023 draft CAC regulation would require internet service providers to prevent the spread of "bad information" on "short-range ad hoc networks", such as Bluetooth, Wi-Fi or other technologies that establish short range networks and provide services for publishing information. [100]

In December 2022, the CAC introduced rules that require technology companies to review all social media posts before they are published and filter out "illegal and harmful" information. [101] In December 2022, the CAC updated the 2017 Regulations on the Administration of Internet Post Comment Services, clarifying the responsibilities of ISPs and other operators to filter out "harmful" content. [102]

Under CAC regulations that took effect in March 2022, platforms' recommendation algorithms must remove "illegal and undesirable content," adhere to "mainstream values," and promote "positive energy." They also impose algorithmic transparency requirements on companies and require them to permit users to decide whether to enable automated content recommendation systems. [103]

CAC regulations, released in draft form in April 2023 and as interim measures in July, require content generated by LLMs to embody "core socialist values" and avoid "information that is violent, obscene, or fake." The rules designate generative-AI providers as online information content producers, subjecting them to CAC censorship regulations. [104] In January 2023, new rules targeting deepfake technology went into effect. Deepfake providers must explicitly label and make traceable any doctored content; must abide by local laws, including national security requirements; and maintain the "correct political direction and correct public opinion orientation." [105] In February 2024, the National Information Security Standardization Technical Committee introduced new rules on basic security requirements for generative artificial intelligence (AI) services that bars datasets containing "more than 5 percent of illegal and harmful information" from being used for training. [106]

Online video broadcasters and live-streamers also are subject to regulations that limit what type of content is allowed to be aired. In March 2021, the NRTA published draft amendments to the Radio and Television Law expanding its coverage to include online video broadcasters and platforms. [107] The amendments specify nine types of banned content, including content that "endangers security," "slanders Chinese culture," or does not help youth "establish the correct world view." [108] In June 2022, the NRTA and the Ministry of Culture jointly issued a new code of conduct for live streamers, podcasters, and other online content producers. The document banned any content that "weakens, distorts or denies the leadership of the CCP." [109]

**B4** 0-4 pts

| **Do online journalists, commentators, and ordinary users practice self-censorship?** | **0** / 4 |
| --- | --- |

Self-censorship among ordinary users and journalists is common and takes place amid an increasing risk of account closures and real-world reprisals including legal penalties for online commentary (see B2, C3, and C7). Self-censorship is exacerbated by nationalistic netizens' intimidation and online harassment of those who they perceive as harming the reputation of China.

The critical role of WeChat in daily life, alongside platform moderators' growing propensity to close accounts rather than delete objectionable posts, has increased pressure on users to self-censor. WeChat is relied on for services including messaging, banking, ride-hailing, ordering food, and booking travel (see B2). [110] Research from the China Dissent Monitor, which is operated by Freedom House, found that owners of verified accounts on Chinese social media platforms may be less likely to post content perceived as challenging the authorities. [111] In October 2022, after photos of a protest on the Sitong Bridge in Beijing went viral, hundreds of users later wrote "confessional letters" apologizing to have their banned Weibo and Wechat accounts reinstated. [112]

Self-censorship is pervasive among members of persecuted groups, especially Uyghurs, whose WeChat activities are closely monitored. Many block relatives living abroad to avoid being detained for having foreign contacts. [113]

Despite these pressures, there are various examples of internet users speaking out on sensitive topics, often using coded language. In April 2023, the light prison sentences handed down to men involved in a prominent human trafficking case sparked outcry. [114] Since the 2020 death of Dr. Li Wenliang, a COVID-19 whistleblower, millions of people have left comments under his final Sina Weibo post, including annually on the anniversary of his death, that often are critical of authorities. [115]

**B5** 0-4 pts

| **Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?** | **0** / 4 |
|---|---|

The government has significant control over digital news media and other information sources. Online discussion is subject to extensive manipulation. [116]

Websites and social media accounts, other than those operated by official news outlets, are not legally allowed to produce news content, though the definition of what constitutes "news" is unclear. Propaganda officials systematically instruct internet outlets to amplify content from state media and downplay news that might generate public criticism of the government. [117] For example, in December 2022, a leaked propaganda directive showed the government ordered state media to portray the abrupt end of the zero-COVID policy as a well-organized, scientifically backed decision. [118] The decision had followed unprecedented mass protests against the policy (see B8).

The Provisions on the Governance of the Online Information Content Ecosystem, implemented in March 2020, [119] categorize online content as either encouraged positive content, discouraged negative content, or illegal content. Encouraged material includes "spreading party doctrine," while negative categories include "excessive celebrity gossip" and sensationalist headlines. According to the rules, the encouraged content must be actively promoted in prominent online locations such as on web portal home pages, pop-up windows, hot topic lists, and default search results. [120] They also call for online content providers to promote officially approved "mainstream values" via algorithms. Most of these actions had been occurring for years, but the provisions consolidated them into a single set of rules. CAC rules introduced in July 2023 order internet companies to crack down on false information. A fact checker introduced by Sina Weibo, similar to community notes on X, has not labelled any Chinese government or state media accounts. [121]

State actors also rely on paid commentators. A December 2020 report examined procurement bids and found that government-funded private companies are hired to post online comments on social media platforms. [122] Paid commentators, historically known as the 50 Cent Party, post progovernment remarks and influence online discussions. [123] Such commentators are known for reporting users who post offending statements, deliberately muddying the facts of particular incidents, and coordinating smear campaigns against government critics. [124] According to a report released in December 2020, a robust government-funded industry of automated online commentating floods social media platforms with desired posts, even under the direction of small local agencies. [125]

A December 2022 Nikkei Asia article reported that nationalist users gained significant traction on Chinese social media in the past decade, amplified by official accounts and government censorship of more moderate content. [126] A document leaked in 2015 revealed hundreds of thousands of "youth league online commentators" in China's higher education institutions, tasked with turning students against supposed "Western" democratic values. [127]

Content manipulation and disinformation campaigns have increasingly extended even to platforms that are blocked in China, including Facebook, [128] Twitter, and YouTube, [129] demonstrating an ability to influence online discourse internationally. [130] In September 2023, a government-backed disinformation campaign on the release of treated wastewater from Japan's ruined Fukushima Daiichi nuclear power plant exaggerated the risks of the discharge and stoked fear and anti-Japanese sentiment. [131] At the same time, scientific-oriented articles debunking these conspiracies were deleted in China. [132]

**B6** 0-3 pts

| **Are there economic or regulatory constraints that negatively affect users' ability to publish content online?** | **0** / 3 |
|---|---|

Growing censorship demands, licensing requirements, and data-localization mandates have made it more expensive to run internet-specific companies, including online news outlets, in China. While large companies have been able to absorb rising operational costs, new and smaller players operate with increasing difficulty. Arbitrary regulatory decisions have also contributed to an unstable investment climate. [133]

Under CAC regulations on managing internet news and information services that came into effect in 2017, [134] only traditional media or state-controlled enterprises may obtain a license to gather or disseminate news online. [135] Regulations from 2016 restrict foreign investment in online publishing and require at least eight full-time editorial or publishing staff members to obtain a license. [136] In addition, CAC rules have made it harder for both independent media and individual bloggers, journalists, and writers to sustain themselves financially. [137] Commercial media outlets such as Caixin, known for relatively aggressive and investigative reporting,

have suffered from falling profits due to censorship and ad hoc directives requiring major news portals and other aggregators to favor state media.

Online self-publishing (individuals or companies that only publish through social media) has been increasingly regulated by the CAC since 2021. A January directive that year required independently operated accounts to obtain a permit and prohibited them from commenting on a list of topics. [138] In November 2022, the CAC released an updated version of Regulations on Comments to Social Media Posts Services, requiring platforms to enforce real-name registration and roll out new content-moderation controls on comment threads (see C4). [139] Following the July 2023 introduction of new regulations for "self-media" accounts, including a requirement that accounts with over 500,000 followers must display their real names, some individuals shut down their accounts. [140]

In October 2021, the CAC released an updated version of the Internet News Information Source List, containing over 1,300 authorized news outlets that can be republished by other news services—four times as many as the CAC's 2016 list. The list removed Caixin and added the social media accounts of state media and government agencies. [141] In October 2021, China's top economic regulator released an amended and revised list for market access that banned private investment in the media, including for the establishment or operation of online news sites. [142]

**B7** 0-4 pts

| **Does the online information landscape lack diversity and reliability?** | **1** / 4 |
|---|---|

China's online information landscape is significantly less diverse than it had been before Xi Jinping came to power in 2012 due to increasing censorship. This strict censorship of critical viewpoints and foreign news sources has also empowered nationalist and conservative voices, which are disproportionately represented in Chinese cyberspace. [143] Nevertheless, the internet still provides narrow avenues for critical discussion and enables the sharing of information on some important social and political issues, particularly when users devise creative workarounds to disguise discussion. [144]

The stringent penalization of groups perceived as a political threat has effectively diminished the online space for civil society in recent years. [145] Groups that worked on issues that were once tolerated online, such as feminist groups and LGBT+ groups, have faced increasing scrutiny from the government and harassment from nationalist accounts, particularly since 2021. [146] Members of marginalized ethnic, religious, and linguistic groups have attempted to use the internet to disseminate banned content or content perceived as problematic by the authorities, but these views are suppressed. For example, Uyghur-language content and relevant news reporting have been heavily censored, and many ordinary Uyghur users have been detained (see B2 and C3), and Tibetan and Uyghur languages banned from some apps. [147] Islamophobic and antisemitic commentary is permitted to circulate widely. [148]

Tens of millions of internet users bypass censorship with circumvention technology or creative workarounds. Although hundreds of VPN services are inaccessible, [149] various options remain available. [150] In late 2022, many Chinese internet users turned to VPNs to circumvent censorship in order to share and access information related to zero-COVID protests (see B8). [151] In 2023, searches for VPNs doubled in China according to data compiled by the news outlet Techopedia, indicating a higher demand for circumvention tools. The surge is likely motivated due to government restrictions on online gaming for young people. [152]

Within the Great Firewall, netizens deploy neologisms, homonyms, and cryptic allusions to substitute for banned keywords. [153] For the past several years, the word "Xinjiang" and the human rights abuses documented there had been taboo on the Chinese internet. Netizens thus used "XJ" and "new jiang" ("xin" means new in Chinese) to try to circumvent censorship. [154] In a similar vein, "JC" was used to reference the police ("jing cha" means police), and "zf" for government ("zhengfu" means government). [155] In July 2022, Sina Weibo announced new rules that sought to restrict the use of homonyms to "spread harmful information." [156]

**B8** 0-6 pts

| | |
|---|---|
| **Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?** | **1** / 6 |

The role of social media in providing a vibrant space for activism in China has waned significantly due to stricter internet controls under Xi Jinping. [157] Growing censorship of popular apolitical platforms such as dating, video-sharing, live-streaming, and blockchain applications in recent years has effectively closed avenues users had used to disseminate information and mobilize. However, people mobilized protests during the coverage period. Data collected for the China Dissent Monitor, which is operated by Freedom House, included 150 distinct instances of online mobilization during the coverage period, spanning issues like environmental pollution, property rights, and sexual harassment. [158]

In November 2022, thousands of people across China held protests against Beijing's zero-COVID policy and CCP rule more generally. The protest was spurred by a fire in Urumqi that killed 10 people that month and spurred by discontent built up over months of strict lockdowns. People took to social media platforms to mourn the victims and share information about protests. Some participants held white sheets of paper as a means of expressing their discontent with the government, and the movement became widely known as the White Paper protests. Censors responded by removing social media posts and accounts sharing news about the protests, and search functions on social media platforms made protest-related information hard to find (see B2). [159] Chinese protesters also used circumvention tools to discuss the protests on global platforms like Facebook, Twitter (now X) and Instagram. [160] Authorities detained scores of protesters across the country (see C3). Online posts discussing their cases or calling for their release were censored. The CAC also ordered social media companies to hire more censors to scrub any references to VPNs. [161]

# C. Violations of User Rights

**C1** 0-6 pts

| | |
|---|---|
| **Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?** | **0** / 6 |

Article 35 of the constitution guarantees freedoms of speech and publication, but such rights are subordinated to the CCP's status as the ruling party. [162] The constitution cannot be invoked in courts as a legal basis for asserting rights. The judiciary is not independent and closely follows party directives, particularly in politically sensitive cases involving freedom of expression. [163]

**C2** 0-4 pts

| **Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?** | **0** / 4 |
|---|---|

Numerous laws and regulations limit online activities, and prosecutors exploit vague provisions to imprison people for their online speech. Trials and hearings typically lack due process. It can take years for cases to move through the court system; the accused are routinely denied bail and frequently face lengthy pretrial detention.

Laws prohibiting offenses including defamation, creating disturbances, illegal commercial activities, and extortion have implications for online speech. [164] Defamation has been interpreted to include "online rumors," content deemed false, or online expression that "seriously harms" public order or state interests. [165] It carries a possible three-year prison sentence under "serious" circumstances, which apply when the content in question receives more than 5,000 views or is reposted more than 500 times. [166] Online messages deemed to incite unrest or protests are subject to criminal penalties under provisions punishing citizens for "picking quarrels and provoking trouble"; the charge is often applied expansively to target expression perceived as critical of or threating to the government. [167]

Crimes such as "subversion" and "separatism," as well as the incitement of such actions, can draw sentences as severe as life in prison. [168] Article 300 of the criminal code punishes "using heterodox religion to undermine implementation of the law" and is often invoked against members of banned religious groups. [169] A 2015 amendment to the criminal code increased the maximum penalties for these crimes from 15 years to life imprisonment [170] and introduced penalties of up to seven years in prison for disseminating misinformation on social media. [171]

A March 2021 amendment to the criminal code stipulated that those who "insult, slander, or infringe the reputation and honor of heroes and martyrs" can be imprisoned for up to three years. [172] A 2021 law bans "slander" of members of the armed forces. [173] In September 2023, authorities proposed amendments to the Public Security Administration Punishments Law to introduce administrative detention penalties and fines for producing or disseminating speech that "hurt the feelings of the Chinese people." [174] The clause "hurt the feelings of the Chinese people" was deleted in a second draft of amendments proposed in June 2024. [175]

The 2015 antiterrorism law bars social media users from sharing information about acts of terrorism or spreading "inhumane" images that could encourage copycat attacks (see B3 and C5). [176] In a guideline jointly introduced in June 2024, China's top judicial, prosecutorial, and public security authorities declared new restrictions on "Taiwan Independence Diehards." Actions such as "tampering with the fact that Taiwan is a part of China" could be considered a crime of secession, with individuals convicted of the crime facing harsh penalties up to the death sentence. [177]

In February 2020, amid the coronavirus outbreak, top judicial and law enforcement agencies released new guidelines for judges, prosecutors, and others working in the legal system urging strong action against crimes seen as weakening disease-control efforts and undermining the CCP's authority. Among the 10 categories of crimes listed for tighter enforcement were "spreading false information and rumors online" and "disrupting social order, especially maliciously attacking the party and government, taking the opportunity to incite subversion of state power, or overthrow of the socialist system." [178]

Some detentions can occur without court approval, [179] and individuals can be detained without trial under poor conditions in drug rehabilitation centers. [180] Chinese law also allows a form of criminal detention termed "residential surveillance at a designated location" [181] where police may hold individuals in secret locations without informing their families or legal counsel for up to six months. [182]

**C3** 0-6 pts

| Are individuals penalized for online activities, particularly those that are protected under international human rights standards? | 0 / 6 |
| --- | --- |

Chinese citizens are regularly jailed for their online activities, and the risk of being detained or imprisoned has increased considerably in recent years. Ordinary users, journalists, human rights activists, bloggers, and religious and ethnic groups are targeted. Rapid advances in surveillance technology and growing police access to user data have helped facilitate the rise in prosecutions (see C5 and C6). [183] An online database updated by an activist posting under the anonymous X (formerly Twitter) account @SpeechFreedomCN, has tracked over 2,500 cases of criminal prosecution for free expression between 2013 and 2024, the vast majority of which are online comments on WeChat, QQ, or other platforms. [184] At least 28 percent of the cases of online dissent recorded in the China Dissent Monitor since 2022 resulted in some form of repression, including 20 cases of detention or arrest. [185]

Journalists in China are frequently imprisoned for their work, online writing, or video posts. According to the Committee to Protect Journalists (CPJ), at least 44 journalists were jailed in China as of December 2023, making the CCP the world's leader in imprisoning journalists that year. [186] Journalist Shangguan Yunkai received a 15-year prison sentence in January 2024 on a number of charges believed to be related to his anticorruption reporting, which he sometimes published on WeChat. [187] Bloggers are also systematically targeted. Australian-Chinese blogger Yang Hengjun received a suspended death sentence in February 2024 on charges of "espionage" that are believed to be related in part to writings that are critical of the government. [188] In June 2024, Huang Xueqin, a prominent blogger and #MeToo activist, was sentenced to five years in prison on the same charge; she was put on trial in September 2023. [189] In February 2023, advocates warned that Huang's physical condition was deteriorating. [190] In February 2023, during the previous coverage period, Ruan Xiaohuan, who had anonymously operated the blog Program Think, was sentenced to seven years' imprisonment for "inciting subversion of state power." [191]

Activists and human rights lawyers have been prosecuted for online activities related to advocating for democratic rights and governance, exposing police abuses, and unionizing efforts, among other topics. In April 2023, a court in

Shandong Province sentenced prominent legal scholar and blogger Xu Zhiyong to 14 years in prison for "subversion of state power." [192] His partner, Li Qiaochu, was sentenced to three years and eight months' imprisonment in February 2024, in part for writing online about torture that Xu had been subjected to. [193] (Li was released in August 2024. [194]) In December 2022, human rights activist Ou Biaofeng received a three-and-a-half-year prison sentence for writing articles for Hong Kong newspapers and for his social media activity, and is expected to be released in September 2024. [195]

Following the November 2023 anniversary of the Urumqi fire and start of the White Paper protests (see B8), independent filmmaker Chen Pinlin was detained on charges of "picking quarrels and provoking trouble" after posting online a documentary he co-produced with footage of the protests; he was formally arrested in January 2024 and faces up to five years in prison. [196] Kamile Wayit, a Uyghur student residing in Henan Province who posted videos relating to the protests on WeChat, was detained in December 2022, when she had returned to Xinjiang, [197] and was sentenced to three years' imprisonment in March 2023. [198]

Members of persecuted religious and ethnic minority groups face particularly harsh treatment for their online activities. In Xinjiang, an estimated one million people have been held in political reeducation camps as of 2018, though exact numbers are difficult to verify. [199] As of 2023, many camps appeared to be decommissioned and closed, and official data showed that some 500,000 Uyghurs, many of them former camp detainees, had received formal prison sentence. [200] For example, Uyghur poet Gulnisa Imin was first held in a reeducation camp before being sentenced to 17.5 years' imprisonment in 2019 on charges of "separatism" for publishing her poetry online, according to news that emerged in 2021. [201] Some Uyghurs were also targeted for communicating with relatives living abroad via WeChat. [202] A police officer confirmed in June 2023 that a university student was sentenced to 13 years in prison in 2017 after the student used a VPN and viewed "illegal information." [203]

Tibetans living outside the Tibet Autonomous Region have also been targeted for sharing information on Chinese social media or overseas websites. Sichuan police detained Tibetan monk Tenzin Khenrap in July 2023 for having a photo of the Dalai Lama on his mobile phone. His social media accounts were shut down, and he remains forcibly disappeared as of February 2024. [204] Tibetan monk Jampa

Choephel was arrested Qinghai Province in March 2024 for sharing an audio clip from the Dalai Lama in a WeChat group in March 2024; he was sentenced to 18 months imprisonment in September. [205]

People in the Tibetan Autonomous Region, a region which is not factored into this report's scores (see Overview), also face arrest and prison terms for their online speech. In August 2022, a teacher in Lhasa was arrested for posts on WeChat and Sina Weibo documenting the harmful implementation of the city's harsh COVID-19 lockdown. [206] In March 2023, a Tibetan woman in the region was detained for sending photos to people outside of Tibet. [207]

Falun Gong practitioners are regularly jailed for posting messages about the spiritual group or human rights abuses on social media, accessing banned websites, and possessing or sharing prohibited VPN technology. [208] In May 2023, Falun Gong practitioner Xu Na's appeal against an eight-year prison sentence was rejected; she had been convicted in 2022 of "organizing or using a cult to undermine implementation of the law" for taking photos of Beijing street scenes during the COIVD-19 pandemic and sharing them online with the Falun Gong publication the *Epoch Times*. [209]

Vague provisions barring online speech have been applied to people using generative AI tools. In May 2023, police in Gansu detained a man on charges of "picking quarrels and provoking trouble" after he allegedly used ChatGPT to generate and post a series of false news reports about a train crash. [210] Separately, the government crackdown on VPNs have led to criminal penalties for their use. In August 2023, a software programmer received a fine of 200 yuan ($30) for using an "unauthorized" VPN to work for an overseas company. The income he had earned at the job totaled 1.1 million yuan ($150,000) and was deemed "illegal," and confiscated by the police. [211]

**C4** 0-4 pts

| **Does the government place restrictions on anonymous communication or encryption?** | **0** / 4 |
|---|---|

Anonymous communication is severely limited. Under 2012 data-privacy legislation and additional 2017 rules, [212] web-service companies are required to register users under their real names and national ID numbers. [213] Guidelines released by

the CAC in June 2022 direct service providers to use real-name registration to prevent users banned for legal or platform policy violations from reregistering and to disclose the geographic locations of users. [214] In March and April 2022, social media platforms like Sina Weibo and Douyin began to display the cities or provinces of China-based users underneath posts. Users outside of China have their country displayed. [215] In December 2022, the CAC released new rules that require ISPs to discontinue service to anyone who had not authenticated their real identity. [216] In June 2023, new rules began requiring "self-media" accounts with over 500,000 followers to display their real name. [217]

Authorities also require SIM card registration, [218] and in December 2019 regulations took effect that require users to have their faces scanned when registering for mobile services. [219] All online gamers are also required to register using their name and phone number, [220] and real-name registration for online literature platforms became mandatory in June 2020, limiting online spaces where many novelists have turned to discuss sensitive subjects in recent years. [221] In January 2023, new CAC regulations went into effect that extend real-name registration requirements to companies that provide image-manipulation services based on machine learning, commonly known as deepfakes. [222] A new law to combat internet and telecoms fraud, a common problem, also introduced further rules on real-name registration for internet services with penalties for noncompliance. [223]

In July 2024, after the coverage period, the CAC and the Ministry of Public Security released draft rules that would introduce a national internet identity system, authorizing the government to issue internet identity numbers linked to people's government identification. The internet identity numbers would be used for the real-name registration mandated across platforms and services. [224]

Authorities in some areas have instructed public Wi-Fi providers to comply with user-registration requirements. [225] Cybercafés check photo identification, record user activities, and at times require facial scans, sometimes in cooperation with law enforcement.

Measures that erode anonymity disproportionately target groups that are perceived as threats to the regime. In Xinjiang, Uyghurs have been required since 2015 to register with their real names when purchasing electronic devices with

storage, communication, and broadcast features. Stores selling such equipment are also required to install software that provides police with real-time electronic records on transactions. [226]

The use of encryption is also severely restricted. The 2015 antiterrorism law requires companies to offer technical support to decrypt information at the request of law enforcement agencies, among other provisions. [227] Regulations for the Administration of Commercial Encryption dating to 1999, and related rules from 2006, separately require a government regulator to approve encryption products used by foreign and domestic companies. [228] In January 2020, a law took effect that requires critical information infrastructure providers to apply for a review by the CAC if their use of encryption technologies is viewed as potentially impacting national security. [229]

In January 2024, Beijing authorities announced they had broken Apple's AirDrop encryption service. [230] Previously, Apple had abandoned different encryption technology it typically uses when storing user data in China, after the Chinese government prohibited the technology (see C6). [231] In February 2023, only two days after it became available, Apple removed the new Damus app— a decentralized platform that allows users to create anonymous accounts and send encrypted messages—from its app store in China at the request of the CAC (see B2). [232]

**C5** 0-6 pts

| **Does state surveillance of internet activities infringe on users' right to privacy?** | **0** / 6 |
|---|---|

Online surveillance is pervasive and highly sophisticated, and privacy protections from government infringement under Chinese law are minimal. The 2021 Personal Information Protection Law permits broad exemption for state entities (see C6). [233] In recent years, the Chinese government has increasingly moved toward big-data integration with the help of private companies, essentially consolidating in various databases a wide array of information on individuals, including their online activities.

One-third of Chinese counties purchased surveillance equipment— including facial recognition–enabled cameras, databases for storing citizen information and

images, and Wi-Fi sniffers to monitor internet traffic—in 2019 alone. [234] Much of the equipment is connected to Project Sharp Eyes, which aims to cover all key public spaces in China by video surveillance. An October 2022 report by Kaspersky Labs uncovered spyware bundled inside an inauthentic version of Tor advertised in China. Tor, a popular anonymizing browser, is blocked in China. [235]

When conducting investigations, the authorities have unfettered access to user communications and data on certain popular platforms, as indicated by reports of users being punished for their presumably private conversations, particularly on WeChat. A June 2022 investigation found that police sought to use international mobile subscriber identity (IMSI)–catchers and Wi-Fi sniffers to extract information about people's mobile phone usage, like social media handles and whether they have downloaded apps deemed problematic. [236] Following the 2022 zero-COVID-related protests, authorities deployed China's extensive surveillance system, including by using mobile phone data and surveillance cameras, to identify and arrest protesters (see B8). [237]

Residents of ethnic minority regions are subject to severely invasive surveillance tactics. In February 2024, rights groups Tibet Watch and Turquoise Roof reported that Beijing has escalated its digital surveillance in Tibet, using a big-data policing system built on technology from the US–based company Oracle. [238] The authorities have ordered the mandatory installation of a government-linked antifraud app on cell phones used in Tibet and Inner Mongolia, among other regions. [239] The software has been found to track users' personal information, leading to an instance where police contacted a user about their browsing activity on oversea news outlets. [240] In 2021, the surveillance technology trade publication IPVM analyzed Xinjiang police data leaked earlier that year, and found Hikvision cameras systematically used to surveil on Uyghurs. [241] A May 2024 IPVM report found that similar cameras were used to monitor Uyghurs outside of Xinjiang. [242] A leaked list of Uyghur detainees examined in a December 2020 report by Human Rights Watch showed how Chinese authorities used big-data technology to arbitrarily detain Muslims in Xinjiang. [243]

Surveillance technologies and policies deployed in one part of China are often later expanded to other parts of the country, with Xinjiang emerging as a particularly important testing ground. [244] Chinese border police were reported to have installed surveillance apps on the phones of some tourists traveling in

Xinjiang in 2019, granting authorities the ability to extract user data and identify politically and culturally sensitive material stored on targeted devices. [245] In 2019, reports emerged that Chinese border officers were beginning to check the photographs, messages, and apps on the mobile phones of anyone arriving in China from Hong Kong for evidence of support for the prodemocracy protest movement there. [246]

Overbroad surveillance and poor data-security practices have facilitated the sale of people's private information on the open market, as with the July 2022 Shanghai police database leaks (see C8). Chinese authorities were able to acquire massive amounts of personal data during the COVID-19 pandemic through the mandatory tracking app Health Code and other applications (see C6).

**C6** 0-6 pts

| **Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy?** | **0** / 6 |
|---|---|

Internet-specific companies are required under numerous laws and regulations to assist the government in monitoring users' online activities. A 2018 rule provides security authorities with broad powers to enter the premises of all internet service companies to inspect and copy any information deemed important to cybersecurity. [247] The regulatory package complemented the 2017 cybersecurity law's requirement that network operators assist police and security agencies with criminal investigations and national security operations. [248]

Government efforts in recent years have tried to regulate how Chinese tech companies collect, share, and store users' data while permitting law enforcement surveillance. The Personal Information Protection Law (PIPL) went into effect in November 2021. [249] The law, which applies to all organizations and individuals in China seeking to access Chinese citizens' data, is the country's first comprehensive legislation about the protection of personal information. However, the law exempts government agencies from data-protection obligations and requires certain companies to store sensitive data on servers located in China, which leaves them vulnerable to government access. [250]

In March 2021, the CAC issued the Provisions on the Scope of Necessary Personal Information for Common Used Mobile Internet Applications, defining what

constitutes "necessary personal information" that mobile internet applications can require consumers to provide. [251] Regulators subsequently alleged that 33 apps—including those from Tencent and Baidu—violated the rules. [252] Separately, in July 2021, authorities asserted that the ride-hailing app Didi illegally collected users' personal information, and the app was pulled from China-based app stores. [253] In December 2021, authorities ordered app stores to remove over 100 apps, including the relatively liberal forum Douban, for data-privacy and security violations, among other offenses. [254]

In May 2020, the National People's Congress passed the country's first civil code, which included a provision that requires an individual's consent for private companies to collect, share, or disclose their digital and biometric data. The provisions came amid growing public concern in China over data collection, hacking, and potential leaks by private companies. [255]

In September 2021, the Data Security Law took effect. [256] The law imposes extensive data-security obligations for businesses. It also regulates data-processing and management activities within China, along with those outside of China that would purportedly harm China's national security or the public interest of Chinese citizens or organizations. It requires companies to obtain approval from the state prior to sharing data with a foreign judicial or law enforcement entity. [257]

The new National Data Administration was established in October 2023 as a part of sweeping restructuring of government agencies. Overseen by the National Development and Reform Commission, it coordinates the sharing, integration, and development of data resources and promotes the construction of data infrastructure. [258]

Other surveillance laws include a 2013 amendment to the criminal procedure code that lays out a vague review process for allowing police monitoring of people's electronic communications, which the Ministry of Public Security permits in many types of criminal investigations. [259] The State Secrets Law obliges telecommunications companies to cooperate with authorities investigating leaked state secrets, or risk losing their licenses. [260]

Individuals or entities that refuse to comply with government requests for surveillance assistance risk detention or criminal punishment. A National Intelligence Law adopted in 2017 states that those deemed to be obstructing national intelligence work can be subject to 15 days of administrative detention and further criminal charges. [261]

Various regulations outline requirements for companies to retain and make user data available to officials. [262] CAC rules issued in 2016 oblige Chinese app providers to register users and keep user-activity logs for 60 days. [263] ISPs are required to retain user information for 60 days and submit it to the authorities upon request, without judicial oversight or transparency. [264]

The 2017 cybersecurity law mandates that internet companies store the data of Chinese residents on servers based in the country, a practice that makes it easier for the government to access user information. [265] In 2018, Apple's iCloud began storing the data of its Chinese users in partnership with Guizhou-Cloud Big Data, a state-run company; [266] a second data center was expected to open in Inner Mongolia. [267] Tencent, which operates the widely used WeChat and QQ social platforms, directly assists the Chinese government with surveillance. [268] The e-commerce giant Alibaba also helps the government with surveillance. [269]

COVID-19-related "health code" apps developed by regional officials in partnership with Alibaba and Tencent, did not adhere to privacy-by-design standards and some shared data automatically with police. [270] In December 2022, the government ended the use of its travel-tracing app. [271] It is unknown what will happen to user data collected by the app. In March 2023, authorities in the city of Wuxi said they deleted one billion pieces of personal data collected since the start of the pandemic; [272] the claim could not be independently verified.

The government also seeks to proactively counter efforts to evade surveillance. In March 2021, the CAC announced that it started talks with technology firms, including ByteDance, Tencent, Alibaba, Xiaomi, and Kuaishou, to explore how to counteract deepfake technologies and voice-changing software, which are often used by activists to elude identification by government authorities. [273]

**C7** 0-5 pts

| Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in relation to their online activities? | 0 / 5 |
| --- | --- |

Cases of extralegal intimidation and violence involving internet users are widespread, including against those already in detention for their online activities. People detained in ordinary criminal cases often experience torture, and political and religious prisoners experience especially severe treatment. [274] Law enforcement officials frequently summon individuals for questioning in relation to online activity, an intimidation tactic referred to euphemistically as being "invited to tea." [275] For example, activists who expressed opposition to the Chinese government's attempts to exercise greater political control over Hong Kong have been summoned. [276]

Activists have experienced restrictions during sensitive political events or other types of intimidation, effectively keeping them away from their normal online activities. [277] In June 2023, rights lawyer Wang Quanzhang said his family had been evicted from 13 homes, electricity cut off, and his son denied school places in an aggressive harassment campaign. [278] In May and June 2023, ahead of the anniversary of the 1989 Tiananmen Square massacre, police restricted the movement and communications of families of Tiananmen victims and activists; activist Chen Siming was detained and later released in Hunan after he refused to delete a Twitter post. [279]

Journalists sometimes experienced physical violence for their work. Activist and journalist Sun Lin was reportedly beaten by police during a raid and died from his injuries in November 2023; he had posted online about videos of anti-Xi protests in the hours before the raid. [280] Police forcibly removed journalists from state broadcaster CCTV from the site of an explosion in March 2024; local authorities later apologized. [281] In May 2023, a reporter with the online outlet Jimu News was beaten by police in Bijie while reporting on the flood-related deaths in the area. [282]

Chinese women often face misogynistic harassment and trolling online, including from state-linked groups such as the Communist Youth League—which used its Weibo account to verbally attacked feminists as "extremists" and a "malignant tumor" that should be removed for calling out the lack of female representation

in a photo series of the history of the CCP. [283] Female researchers, journalists, and activists of Asian descent across all major social media platforms abroad have also faced surveillance, intimidation, and disinformation campaigns from China-based actors. [284]

Members of marginalized religious and ethnic minority groups are among the internet users most vulnerable to extralegal detention, torture, and killing. In Xinjiang, some of the estimated one million Uyghurs and other Muslims have been taken to extralegal reeducation camps because of online activities. [285] Tibetans also face physical violence for their online activity. Tibetan advocate Tashi Wangchuk was attacked in the Tibet Autonomous Region (a region that is not covered by this report, see Overview) by a group believed to be connected to state authorities in August 2023 after posting a photo on social media. [286] In 2019, Tibetan monk Choegyal Wangpo was arrested and severely beaten after police found his phone at a café, which contained WeChat messages to monks in Nepal. [287]

Chinese authorities have increasingly resorted to transnational repression to suppress online criticism of the government originating from outside China. In August 2023, Laos-based Chinese activist Qiao Xinxin surfaced in detention in Hunan Province after disappearing from Laos shortly after he launched an online anticensorship campaign called "BanGFW Movement". [288]

**C8** 0-3 pts

| **Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?** | **0**/3 |
|---|---|

China is a significant origin point of global cyberattacks. Attacks known to have originated in China can rarely be linked directly to the state, and much of the activity appears decentralized and uncoordinated. However, many attacks employ sophisticated technology, and experts believe that Chinese military and intelligence agencies either sponsor or condone technical attacks on political targets both within and outside China.

In April 2024, two overseas Chinese dissident accounts described receiving phishing links on X; [289] the method was similar to methods described in leaked

files from a Chinese security company in February 2024 that targeted domestic and overseas users. [290] The Chinese security company I-soon sold its services to the Ministry of Public Security to surveil Chinese citizens in the country and abroad, according to documents leaked in February 2024. [291]

Mass surveillance also leaves people's personal information vulnerable to breaches. In July 2022, hackers claimed to have accessed a Shanghai police database that contained records associated with one billion Chinese citizens. The database reportedly contained information including names, addresses, national ID numbers, and criminal records. [292] One media outlet contacted a small number of people listed in the database and verified their records were authentic. [293]

## *Footnotes*

1 "The 53nd Statistical Report on Internet Development in China", March 2024, page 17, http://www.gov.cn/xinwen/2022-09/01/content_5707695.htm https://www.cnnic.com.cn/IDR/ReportDownloads/202405/P020240509518443205...

2 Charlotte Gao, "China's Great Firewall: A Serious Pain in the Neck for European and US Companies," The Diplomat, June 21, 2018, https://thediplomat.com/2018/06/chinas-great-firewall-a-serious-pain-in....

3 "China Median Speeds," Ookla Speedtest Global Index, accessed August 2, 2024, https://www.speedtest.net/global-index/china.

4 Broadband Development Alliance, "中国宽带速率状况报告" [China Broadband Speed Status Report], Issue 34, Q4 2023, April 21, 2024, page 6, https://web.archive.org/web/20220524140855/http://www.chinabda.cn/Site/...

5 Juan Pedro Tomas, "China ends 2023 with 3.38 million 5G base stations", January 23 , 2024, https://www.rcrwireless.com/20240123/network-infrastructure/towers/chin... .

More footnotes

**On China**

See all data, scores & information on this country or territory.

See More ›

*Country Facts*

Population

**1,412,175,000**

Global Freedom Score

**9** /100 **Not Free**

Internet Freedom Score

**9** /100 **Not Free**

Freedom in the World Status

**Not Free**

Networks Restricted

**Yes**

Social Media Blocked

**Yes**

Websites Blocked

**Yes**

Pro-government Commentators

**Yes**

Users Arrested

**Yes**

*In Other Reports*

Freedom in the World 2024

*Other Years*

2023

## Be the first to know what's happening.

Join the Freedom House weekly newsletter

Subscribe

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES
info@freedomhouse.org

PRESS & MEDIA
press@freedomhouse.org